UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN
AT LAW AND IN ADMIRALTY

UNITED STATES OF AMERICA,

Plaintiff,

v. Case No.

APPROXIMATELY 459,611.859199 TETHER (USDT) CRYPTOCURRENCY FROM CRYPTOCURRENCY ADDRESS ENDING IN Vs7by2cS,

Defendant.

VERIFIED COMPLAINT FOR CIVIL FORFEITURE IN REM

The United States of America, by its attorneys, Richard G. Frohling, Acting United States Attorney for the Eastern District of Wisconsin, and Elizabeth M. Monfils, Assistant United States Attorney for this district, alleges the following in accordance with Supplemental Rule G(2) of the Federal Rules of Civil Procedure:

Nature of the Action

1. This is a civil action to forfeit property to the United States of America, under 18 U.S.C. §§ 981(a)(1)(A) and 984 and 21 U.S.C. § 881(a)(6), for violations of 18 U.S.C. §§ 1956, 1957, and 1960 and 21 U.S.C. § 841.

The Defendant In Rem

2. The defendant property, approximately 459,611.859199 Tether (USDT)[1] cryptocurrency from cryptocurrency address ending in Vs7by2cS, was seized on or about October 31, 2024, in Road Town, Tortola, British Virgin Islands.

[1] Tether, often referred to by its currency code of USDT, is a stablecoin cryptocurrency with a value meant to mirror the value of the U.S. dollar. USDT tokens are backed by offshore banks. Offshore banks offer

3. The Drug Enforcement Administration seized the defendant property, approximately 459,611.859199 Tether (USDT) cryptocurrency from cryptocurrency address ending in Vs7by2cS, pursuant to seizure warrant 24-MJ-243 issued by United States Magistrate Judge William E. Duffin in the Eastern District of Wisconsin on October 31, 2024.

4. The defendant property is presently in the custody of the United States Marshal Service in Arlington, Virginia.

Jurisdiction and Venue

5. This Court has subject matter jurisdiction over an action commenced by the United States under 28 U.S.C. § 1345, and over an action for forfeiture under 28 U.S.C. § 1355(a).

6. This Court has *in rem* jurisdiction over the defendant property under 28 U.S.C. § 1355(b).

7. Venue is proper in this judicial district under 28 U.S.C. § 1355(b)(1) because the acts or omissions giving rise to the forfeiture occurred, at least in part, in this district.

Basis for Forfeiture

8. The defendant property, approximately 459,611.859199 Tether (USDT) cryptocurrency from cryptocurrency address ending in Vs7by2cS, is subject to forfeiture under 21 U.S.C. § 881(a)(6) because it is traceable to, and is therefore proceeds of, distribution of controlled substances in violation of 21 U.S.C. § 841.

9. The defendant property, approximately 459,611.859199 Tether (USDT) cryptocurrency from cryptocurrency address ending in Vs7by2cS, is also subject to forfeiture under 18 U.S.C. §§ 981(a)(1)(A) and 984 because (1) it was involved in, or is traceable to funds involved in, money laundering transactions and a conspiracy to engage in money laundering in

fewer charges for operation and tax benefits, but they are not always fully secure like the FDIC-insured U.S. banks.

violation of 18 U.S.C. §§ 1956 and 1957; and (2) it was involved in, or is traceable to funds involved in, unlicensed money transmitting in violation of 18 U.S.C. § 1960.

Facts

10. Cocaine is a Schedule II controlled substance under 21 U.S.C. § 812.

Background

11. Drug trafficking organizations ("DTOs") generate large amounts of cash proceeds in the United States and elsewhere. In order to repatriate their cash proceeds from the United States and other countries back to their country of origin where they can be used by the DTO members, DTOs often employ professional money launderers. For a fee, professional money launderers provide the DTO with currency in the DTO's native country in exchange for bulk currency in the country where the DTO's narcotics are distributed.

12. Professional money launderers use a variety of methods to accomplish their goals, including trade-based money laundering, bulk currency smuggling, and virtual currency trading.

13. Virtual currency, also known as cryptocurrency, is generally defined as an electronically sourced unit of value that can be purchased with, sold for, or used as a substitute for fiat currency (i.e., currency created and regulated by a government). Cryptocurrency is not issued by any government, bank, or (with limited exceptions) companies. It is instead generated and controlled through computer software operating on a decentralized peer-to-peer network.

14. Cryptocurrency can be quickly transmitted directly between parties and across national borders, without the need for a facilitating third party like a traditional financial institution. Many cryptocurrencies, including Bitcoin and Tether, operate via a "blockchain," a record (or ledger) of every transaction ever conducted that is distributed throughout the network. The blockchain will not list the names of parties to the transaction but will list the date and time

of the transaction, the originating and receiving public address, and how much cryptocurrency was transferred.

15. Based on their training and experience, and their knowledge and information garnered from money launderers in this case and similar cases, agents know that cryptocurrency transactions are often used to launder the proceeds derived from narcotic traffickers. More specifically,

A. Narcotics traffickers in source countries (e.g., Mexico and Colombia) provide narcotics to consumer countries (e.g., the United States).

B. The bulk currency proceeds derived from the sale of these narcotics are then returned to the narcotics traffickers within the source countries using various methods, including the use of cryptocurrencies. In this case, the narcotics traffickers often contacted brokers, or professional money launderers, who were responsible for collecting the bulk currency within the consumer countries and depositing the currency into the U.S. banking system.

C. The brokers often then paid out the narcotics traffickers in fiat currency within the source countries, minus a commission, and sold the cryptocurrency to a separate "crypto" broker. The commission fee was generally between three percent and five percent.

D. The cryptocurrency broker may have then conducted a series of cryptocurrency transactions across multiple cryptocurrency exchanges using an array of methods (e.g., cryptocurrency scrambler) in an effort to obfuscate the true origin of the money. The cryptocurrency brokers often then sold the cryptocurrency in the "black market" in exchange for various fiat currencies.

International drug trafficking and money laundering organization

16. Agents identified a drug trafficking and money laundering organization ("DTMLO") that collected drug proceeds from drug trafficking organizations that operated in the Milwaukee, Wisconsin, area.

17. Members of this DTMLO also operated in cities throughout the United States at the direction of members of Mexican drug cartels, specifically the Sinaloa Cartel and the Jalisco New Generation Cartel. Money brokers operating in Mexico and Colombia arranged for couriers

operating throughout the United States to pick up drug proceeds from multiple drug trafficking organizations. The drug proceeds were then transferred to other money couriers or deposited into bank accounts or cryptocurrency wallets used by drug traffickers and money launderers to launder proceeds of drug sales.

18. Individuals connected with this criminal and financial investigation in the Eastern District of Wisconsin included individuals having the initials J.S.A., L.S., and E.R., among others.

Identification of individual having the initials J.S.A.

19. In approximately November 2023, agents began investigating J.S.A.

20. Based on their investigation to date, agents believe that J.S.A. is a money launderer specializing in cryptocurrency and the head of the DTMLO.

21. Two confidential sources ("CS-1" and "CS-2") provided information to agents about a Colombia-based money broker involved in laundering drug proceeds for Mexico-based drug traffickers. CS-1 and CS-2 provided phone numbers and other information to agents about this broker.

22. Agents consulted law enforcement databases and identified this broker as J.S.A. CS-1 subsequently viewed a photo of J.S.A. and identified J.S.A. as the Colombia-based money broker.

Cryptocurrency scheme and drug nexus to bulk currency

23. From December 2023 through July 2024, agents conducted four pickups of bulk currency – suspected drug trafficking proceeds – at the request of J.S.A. In total, over $700,000 in currency was picked up, with the majority of that being sent to cryptocurrency addresses provided by J.S.A. As part of these contracts, J.S.A. provided CS-1 and CS-2 with several USDT deposit addresses to send USDT.

24. In November 2023, J.S.A. began to provide money laundering contracts to CS-1 and CS-2. J.S.A. initially requested that money be picked up in Baltimore, Maryland; Houston, Texas; Dallas, Texas; and Denver, Colorado. CS-1 and CS-2 agreed to assist J.S.A. with these money laundering contracts.

A. In these contracts, CS-1 and CS-2, at the direction of agents, organized pickups of bulk currency – suspected drug trafficking proceeds – throughout the United States.

B. The currency was then deposited into undercover Attorney General Exempted Operation accounts, which are undercover accounts that provide the Drug Enforcement Administration ("DEA") the authority to conduct undercover financial transactions to infiltrate and dismantle DTMLOs.

C. After the bulk currency was deposited into undercover bank accounts, it was converted to a stablecoin[2] and sent to cryptocurrency deposit addresses provided by J.S.A.

Money pickup in Dallas, Texas

25. In November 2023, J.S.A. requested that CS-1 and CS-2 coordinate the pickup of $60,000 in bulk United States currency – suspected drug trafficking proceeds – in the Dallas, Texas, area and arrange for the funds to be sent to J.S.A. via cryptocurrency. Agents coordinated with DEA-Dallas investigators to arrange for an undercover Task Force Officer ("UC") to pick up the currency. DEA-Dallas investigators provided agents with a phone number, to be used by the UC, and a $1.00 bill serial number to be used to verify the pickup.[3] Agents provided this information to CS-1 and CS-2, who then provided it to J.S.A.

[2] Stablecoins are cryptocurrencies whose value is pegged to that of another currency, commodity, or financial instrument. Stablecoins aim to provide an alternative to the high volatility of the most popular cryptocurrencies, including Bitcoin (BTC), which has made crypto investments less suitable for everyday transactions.

[3] Based on their training and experience, agents know that money launderers verify they are coordinating with the correct money courier by comparing a serial number of a dollar bill that was previously arranged as part of the money pickup.

26. Several days later, the UC received a phone call from an unknown male using a Texas phone number. During that call, the UC and the male agreed to meet so that the male could deliver "papers," a code word for money, to the UC.

27. In December 2023, the UC and the male met in a parking lot in Dallas, Texas. The male asked for the $1.00 bill bearing the serial number he had been provided. The UC provided the male with the $1.00 bill bearing the serial number previously provided to J.S.A. The male then asked the UC to sign the bill, and the male then took a photo of the bill for confirmation. The male then retrieved a backpack from his vehicle. The backpack contained bundles of United States currency. The UC and the male then departed the location.[4]

28. The currency was transported to a bank where it was deposited into a DEA-Milwaukee undercover account. An official count determined that $60,000 had been delivered. Agents then took a three percent commission ($1,800) for laundering the funds and sent $58,200 to an undercover cryptocurrency exchange account. The funds were converted to USDT cryptocurrency and sent to a cryptocurrency address provided by J.S.A. J.S.A. later confirmed receipt of the cryptocurrency.

29. Based on their investigation to date, agents believe the currency delivered in December 2023, was proceeds of drug trafficking.

30. Based on their investigation to date, agents also believe that the cryptocurrency sent to J.S.A. following the December 2023 money pickup would be further laundered as proceeds of drug trafficking.

[4] The UC recognized the male as someone who had also delivered bulk currency to the UC in September 2023.

Money pickup in Milwaukee, Wisconsin

31. In February 2024, J.S.A. contacted CS-1 and CS-2 and requested the pickup of $250,000 in bulk currency – suspected drug trafficking proceeds – in Milwaukee, Wisconsin. CS-1 and CS-2 contacted agents, who provided CS-1 and CS-2 with a $1.00 bill serial number and a telephone number to be used by a UC.

32. A few days later, the UC received a series of text message from a Mexico-based phone number. The caller confirmed the $1.00 bill serial number and invited the UC to chat using WhatsApp. The UC was unable to chat using WhatsApp. Agents notified CS-1 and CS-2 of this information. CS-1 and CS-2 contacted J.S.A., who confirmed that conversations regarding the money pickup could take place using regular calls and text messages.

33. The following day, a male called the UC from the same number. The UC and the male agreed to meet. The UC confirmed that the male was in the Milwaukee area and asked the male how many "invitations" (how much money) the male had. The male stated he had "250 centimeters," which the UC understood to be $250,000. The male then stated he had between 250 and 300, and by Friday it would be "300 centimeters," a reference to $300,000.

34. On the date of the arranged meeting in February 2024, the UC went to a parking lot where the UC had agreed to meet the male. A short time later, the UC saw a gray 2016 Dodge Caravan, bearing Wisconsin license plates ATT-3XXX,[5] stop close to the UC's vehicle. These license plates were registered to an individual having the initials L.S. and having an address in Milwaukee, Wisconsin. The UC received a call from the male. The male asked for the UC's location. The UC confirmed that UC was at the location and asked if the male's associate was in a

[5] Throughout this complaint, certain information has been redacted using the letter "X" as a means of avoiding the revelation of any personal information.

minivan. The male replied in the affirmative. The UC indicated that UC saw the associate and would verify the $1.00 bill serial number with the associate.

35. The UC saw the male driver of the Dodge Caravan, later identified as L.S., open the rear sliding door of the Dodge Caravan. L.S. then approached the UC's vehicle and entered the front passenger seat. The UC provided L.S. with the $1.00 bill serial number. L.S. appeared to be comparing the serial number to a photo on L.S.'s phone or sending the serial number in a message. L.S. then told the UC that L.S. would give the UC the money. L.S. exited the UC's vehicle and returned to the Dodge Caravan. L.S. opened the passenger-side sliding door of the Dodge Caravan and retrieved a brown and orange Home Depot box, partially wrapped in duct tape. L.S. returned to the UC's vehicle and placed the box on the front passenger floorboard. L.S. then closed the door to the UC's vehicle and returned to the Dodge Caravan. The UC and L.S. then departed the area.

36. The UC was followed to a predetermined location. Upon arrival at the predetermined location, agents met with the UC and opened the Home Depot box. The box contained 30 numbered (1 through 30) duct-tape-wrapped packages believed to contain United States currency. Agents transported the currency to the DEA-Milwaukee District Office where the duct tape was removed from the packages. Each package contained United States currency wrapped in rubber bands, then wrapped in plastic, and finally wrapped in the duct tape.[6] The currency totaled approximately $300,000. Agents deposited those funds into a DEA-Milwaukee undercover bank account. After removing a small commission fee, agents sent the remaining $290,500 to a DEA-Milwaukee undercover cryptocurrency exchange account. The funds were converted to USDT cryptocurrency and sent to a cryptocurrency address provided by J.S.A. J.S.A. later confirmed receipt of the cryptocurrency.

[6] Based on their training and experience, agents believe this wrapping was done to conceal the odor of controlled substances on the currency.

37. In March 2024, agents established surveillance at L.S.'s residence and later saw a vehicle registered to L.S. arrive at the location. While conducting surveillance of that vehicle, agents observed a black BMW SUV, bearing Illinois temporary registration 008134XXX, park in front of the garage. The black BMW was registered to individuals having the initials Y.C. and J.P. at an address in Milwaukee, Wisconsin.[7] Agents saw the garage door open but did not see anyone exit the vehicle or the garage. Due to heavy tint on the black BMW, agents were unable to see the driver or any passengers. The black BMW drove around the parking lots (L.S. resided in a multi-building apartment complex with multiple parking lots) and appeared to be conducting counter-surveillance multiple times. The black BMW eventually left the area. Since that time, agents have conducted surveillance of L.S. and J.P. on several occasions and have observed them drive erratically or utilize counter-surveillance techniques to determine if they are being followed. L.S. has also followed surveillance vehicles on several occasions in attempts to determine who is inside the vehicles.[8] Phone records also show that L.S. was in contact with J.P. as well as other numbers linked to drug trafficking investigations in the Milwaukee, Wisconsin, area.

38. Based on their investigation to date, including L.S.'s contacts with J.P., a known cocaine trafficker, and other phone numbers associated with known drug traffickers; the manner in which the currency received from L.S. was packaged; the manner in which the currency was delivered; the coordination involving the $1.00 bill serial number; and the coordination of the money delivery by someone using a Mexican phone number, agents believe the currency delivered by L.S. was proceeds of drug trafficking.

[7] Agents are aware that J.P. was previously identified as a cocaine trafficker in the Milwaukee, Wisconsin, area.

[8] Based on their training and experience, agents know that these are all tactics used by drug traffickers who are attempting to determine if they are being followed by law enforcement.

39. Based on their investigation to date, agents believe that the cryptocurrency sent to J.S.A. following the February 2024 money pickup would be further laundered as proceeds of drug trafficking.

Money pickup in Johnson Creek, Wisconsin

40. In February 2024, J.S.A. contacted CS-1 and CS-2 and requested the pickup of $169,000 in bulk currency – suspected drug trafficking proceeds – in Madison, Wisconsin. CS-1 and CS-2 contacted agents, who provided CS-1 and CS-2 with a $1.00 bill serial number and a telephone number to be used by a UC.

41. During the following weeks, the UC was in contact with a male, later identified as an individual having the initials E.R. They arranged to meet for the money transfer in Johnson Creek, Wisconsin.

42. In March 2024, in anticipation of the arranged money transfer, DEA-Milwaukee and DEA-Madison agents established surveillance at a parking lot in Johnson Creek, Wisconsin. A short time later, the UC arrived in the parking lot. Approximately 15 minutes later, a black 2023 Dodge Ram truck, bearing Nevada license plate LV5XXX, arrived and parked by the UC's vehicle. The Dodge Ram was registered to E.R. with an address in Las Vegas, Nevada.

43. Agents saw E.R. exit the driver's door of the Dodge Ram and enter the front passenger seat of the UC's vehicle. The UC handed E.R. a $1.00 bill. E.R. appeared to be taking a photograph of the $1.00 bill or comparing the serial number to a photo on his phone while engaging in small talk with the UC. Approximately one minute later, E.R. exited the UC's vehicle and retrieved a blue duffle bag from the rear driver's-side door of the Dodge Ram. E.R. then put the duffle bag on the front passenger-side floorboard of the UC's vehicle. E.R. then re-entered the driver's seat of the Dodge Ram. The UC and E.R. then departed the area.

44. The UC was followed to a predetermined location where agents opened the blue duffle bag. The bag contained a large amount of United States currency wrapped in rubber bands. The bag also contained several dryer sheets.[9] The currency totaled over $250,000. Agents deposited those funds into a DEA-Milwaukee undercover bank account. After removing a small commission fee, agents sent the remaining $250,435 to a DEA-Milwaukee undercover cryptocurrency exchange account. The funds were converted to USDT cryptocurrency and sent to a cryptocurrency address provided by J.S.A. J.S.A. later confirmed receipt of the cryptocurrency.

45. After the March 2024 money transfer was completed, DEA-Madison agents continued surveillance of E.R. until E.R. entered an apartment in Verona, Wisconsin. DEA-Madison agents then initiated an investigation into the drug trafficking and money laundering activities of E.R. DEA-Madison agents obtained court authorization to track the Dodge Ram truck driven by E.R. as well as E.R.'s cellular phone. Using that information, agents identified a storage unit used by E.R. to store drugs and/or money. DEA-Madison agents also confirmed that E.R. traveled to Sinaloa, Mexico, by plane from March 27, 2024, until April 5, 2024.

46. In May 2024, DEA-Madison agents interviewed a confidential source ("CS-3"). CS-3 stated, among other things, the following:

A. CS-3 had known E.R. for approximately five years and had been purchasing kilogram quantities of cocaine from E.R. for approximately three years.

B. CS-3 typically purchased five kilograms of cocaine per month from E.R. for $20,000 to $22,000 per kilogram.

C. E.R. lived in a top-floor apartment in Verona, Wisconsin.

D. CS-3 had purchased cocaine from E.R.'s residence on several occasions and had previously observed more kilograms of cocaine at E.R.'s residence than what CS-3 was purchasing.

E. E.R. drove a black Dodge Ram and a gray Honda sedan.

[9] Based on their training and experience, agents believe the dryer sheets were placed in the bag to mask any odor of controlled substances on the currency.

F. CS-3 believed the last time that CS-3 had purchased cocaine from E.R. was sometime during the week of April 15, 2024, when CS-3 purchased two kilograms of cocaine from E.R. at E.R.'s residence. CS-3 had then paid E.R. approximately $18,000 on or around April 30, 2024, but CS-3 still owed E.R. approximately $25,000 for the cocaine.

47. On June 6, 2024, CS-3 informed agents that E.R. told CS-3 that E.R. still had approximately one kilogram of cocaine that E.R. could give to CS-3. Agents directed CS-3 to arrange to meet with E.R. to obtain the kilogram of cocaine.

A. On June 6, 2024, tracking information showed that E.R. traveled to E.R.'s storage unit before returning to E.R.'s residence. According to the CCTV, at approximately 9:31 p.m., E.R. entered E.R.'s residence carrying a duffle bag and a Pacifico Clara beer box.

B. Before the meeting between E.R. and CS-3, investigators searched CS-3 and CS-3's vehicle for weapons and contraband, which yielded negative results. CS-3 was provided with an audio/video recording device. Agents established surveillance at E.R.'s residence, the pre-arranged meeting location, in anticipation of the controlled cocaine purchase. A short time later, CS-3 arrived at E.R.'s residence and went inside. Approximately twenty minutes later, surveillance agents saw CS-3 exit E.R.'s residence carrying a large plastic shopping bag. Agents saw CS-3 depart in CS-3's vehicle shortly thereafter. Immediately following the controlled purchase, agents met with CS-3, at which time CS-3 turned over to agents approximately one kilogram of suspected cocaine[10] received from E.R. and the audio/video recording device.

C. CS-3 provided the following information to agents regarding CS-3's meeting with E.R.: E.R. retrieved the kilogram of cocaine from a Target shopping bag from inside of the closet near the front entrance of E.R.'s residence. The kilogram was wrapped in duct tape. E.R. unwrapped the kilogram and weighed it for CS-3 before putting it in a Ziploc bag. E.R. then put the Ziploc bag (containing the cocaine) inside of the money bag and gave it to CS-3. E.R. washed the original packaging the kilogram was in (duct tape, plastic wrapping) with soap and water to remove any fingerprints. CS-3 told E.R. that CS-3 would throw away the kilo wrappers with other trash that E.R. had given to CS-3.

[10] In July 2024, the cocaine that CS-3 received on June 6, 2024, from E.R. was analyzed by the DEA Laboratory and identified as cocaine hydrochloride. The cocaine weighed approximately 969.3 grams and the purity was approximately 87 percent.

48. Based on their investigation to date, including the manner in which the currency received from E.R. in March 2024 was packaged; the manner in which the currency was delivered; the coordination involving the $1.00 bill serial number; and the DEA-Madison investigation that showed E.R. is a cocaine trafficker and money launderer, agents believe the currency delivered by E.R. was proceeds of drug trafficking.

49. Based on their investigation to date, agents believe that the cryptocurrency sent to J.S.A. following the March 2024 currency pickup would be further laundered as proceeds of drug trafficking.

Money pickup in Bolingbrook, Illinois

50. In July 2024, J.S.A. contacted CS-1 and CS-2 and requested the pickup of $100,000 in bulk currency – suspected drug trafficking proceeds – in Chicago, Illinois. DEA-Chicago agents provided DEA-Milwaukee agents with an undercover phone number and the serial number of a $1 bill. Later that day, a DEA-Chicago UC received a text message from a Mexico-based telephone number used by an individual having the initials R.S.,[11] that stated, "Hola hola parte Andrea Chica Toke 8479H," which translates to "Hello hello on behalf of Andrea girl Token 8479H." The alphanumeric combination "8479H" are the last five numbers of the $1 bill serial number that was provided to J.S.A. by CS-1. The UC and R.S. spoke about the serial number and ultimately agreed to meet.

51. On the date of the arranged meeting in July 2024, the UC again communicated with R.S., and they agreed to meet at 11:00 a.m. in Bolingbrook, Illinois. R.S. told the UC that a female courier would be meeting the UC and that the courier would be driving a blue Volkswagen. A

[11] During another ongoing DEA investigation, agents identified the user of this Mexican phone number as R.S. A voice comparison of the Spanish-speaking male using the phone in contact with the UC was also determined to be R.S. R.S. was arrested on December 7, 2023, for possession with intent to distribute approximately one kilogram of cocaine in Chicago, Illinois, and was later suspected to have fled the United States, presumably to Mexico.

short time later, surveillance units saw a blue Volkswagen arrive in the parking lot of a restaurant. R.S. sent a message to the UC that the courier had arrived. The UC asked R.S. to direct the courier to a different part of the parking lot. The blue Volkswagen then drove to the location provided by the UC. Surveillance units saw a female, later identified as an individual having the initials A.V.M., exit the driver's seat of the Volkswagen carrying a bag. A.V.M. entered the front driver's seat of the UC's vehicle. While in the vehicle, A.V.M. delivered the bag to the UC and exited UC's vehicle shortly thereafter.

52. The UC drove to a predetermined location where the bag was photographed and found to contain a quantity of rubber-banded currency in vacuum packaging, along with a quantity of loose currency.[12]

53. Based on their investigation to date, including the manner in which the currency received from A.V.M. in July 2024 was packaged, and the fact that R.S. – a previously arrested cocaine trafficker – coordinated the money pickup, agents believe the currency was proceeds of drug trafficking.

54. The currency was transported to a bank where an official count revealed the bag contained $100,000 in currency. The money was deposited into a DEA-Milwaukee undercover bank account. After removing a small commission fee, DEA-Milwaukee agents transferred the remaining $97,000 to an undercover cryptocurrency account. Agents then purchased cryptocurrency in the amount of 97,000.97001 USDT.

55. J.S.A. provided USDT deposit address ending in 805e4fbd ("address 805e4fbd") as the destination to which the funds were to be sent. On July 18, 2024, agents sent the 97,000.97001 USDT to address 805e4fbd with a fee of 4.875559 USDT. Ultimately,

[12] Based on their training and experience, agents know that drug traffickers package currency in vacuum packaging in an attempt to conceal the odor of narcotics that might be associated with the currency.

96,996.094451 USDT arrived at address 805e4fbd. This transaction was completed on the Ethereum blockchain on July 18, 2024, at 3:12 p.m. (UTC).

56. Address 805e4fbd has been involved in other money pickup activity, including the following:

A. In July 2022, a money pickup was conducted in Chicago, Illinois, in which $49,300 was received and deposited into a DEA-Milwaukee undercover bank account. Of that, $47,821 was then transferred to an undercover cryptocurrency exchange account, and 47,812.4 USDT was sent from the undercover account to address 805e4fbd.

B. In September 2022, a money pickup was conducted in New York, New York, in which $104,000 was received and deposited into a DEA-Milwaukee undercover bank account. Of that, $100,880 was then transferred to the undercover cryptocurrency exchange account, and 108,849.7 USDT was sent from the undercover account to address 805e4fbd.

C. In January 2024, two money pickups were conducted in Chicago, Illinois, and Harper Woods, Michigan. Following these pickups and conversion of the currency to cryptocurrency, a series of transactions occurred and 4,370 USDT arrived at address 805e4fbd.

D. In February 2024, a money pickup was conducted in Milwaukee, Wisconsin (described in paragraphs 31 - 39), in which around $300,000 was received and deposited into a DEA-Milwaukee undercover bank account. Of that, $290,500 was then transferred to the undercover cryptocurrency exchange account, and 145,246.935 USDT was sent from the undercover account to address 805e4fbd.

E. In March 2024, a money pickup was conducted in Johnson Creek, Wisconsin (described in paragraphs 40 - 49), in which over $250,000 was received and deposited into a DEA-Milwaukee undercover bank account. Of that, $250,435 was then transferred to the undercover cryptocurrency exchange account, and 124,996.925153 USDT was sent from the undercover account to address 805e4fbd.

F. In October 2024, money pickups were conducted in Chicago, Illinois, and Boston, Massachusetts. Following these pickups and conversion of the currency to cryptocurrency, a series of transactions occurred and 1,000 USDT arrived at address 805e4fbd.

57. Agents determined that address 805e4fbd was a deposit address belonging to KuCoin, a cryptocurrency exchange. KuCoin records did not include the name of an account

holder for address 805e4fbd but did provide email address johnsoXXXXX@gmail.com and a Colombia-based phone number of 57-32332XXXXX. CS-1 later identified the user of the KuCoin account as an individual having the initials J.S., a resident of Cali, Colombia. CS-1 stated that J.S. was involved in the buying and selling of cryptocurrency.

58. KuCoin records show that on July 18, 2024, at 4:15 p.m. (UTC), J.S. sent 95,000 USDT from address 805e4fbd to address ending in GEvrDQ5K, hereinafter "Related Address A."[13]

59. Blockchain analysis shows that following the receipt of the 95,000 USDT, Related Address A divided the funds between two separate addresses. In one of the transfers, which occurred on July 18, 2024, at 5:03 p.m. (UTC), 44,512 USDT were sent to address ending in jm7B4CUn, hereinafter "Related Address D."[14] Following the receipt of 44,512 USDT, Related Address D divided the funds and sent two transfers.

A. In the first transfer from Related Address D, which occurred on July 18, 2024, at 5:06 p.m. (UTC), 29,000 USDT was sent to address ending in K8tbWtoo, hereinafter "Related Address E," an address associated with OKX exchange.

B. In the second transfer from Related Address D, which occurred on July 18, 2024, at 5:08 p.m. (UTC), the remaining 15,512 USDT were transferred to address ending in Vs7by2cS, the address from which the defendant property was seized ("Subject Address Vs7by2cS").

[13] This transaction took place about one hour after agents sent 97,000.97001 USDT to address 805e4fbd – as directed by J.S.A. – following the $100,000 money pickup in Illinois on July 18, 2024, as noted in paragraph 55.

[14] The remaining USDT was transferred out of Related Address A through a series of other account addresses.

Identification of money laundering network

60. Agents analyzed Subject Address Vs7by2cS and Related Addresses A through H described herein (collectively, the "Related Addresses"), and identified a network of addresses that appear to be acting in concert to transfer funds related to suspected money laundering transactions. The transactions conducted by Subject Address Vs7by2cS and the Related Addresses appear to lack a legitimate business or investment purpose. Several addresses within this network activated other network addresses, indicating the addresses were used by the same people or others acting within the same money laundering network, as detailed below. Additionally, funds were frequently exchanged between the addresses, further indicating that the owners of the addresses were working together to further obfuscate the source and destination of funds involved in suspected money laundering activities.

61. Blockchain records indicate that Subject Address Vs7by2cS and the Related Addresses are unhosted wallets, meaning they are not connected to a virtual currency exchange that would require Know Your Customer (KYC) information.[15] Based on their training and experience, and the investigation to date, agents know that money launderers commonly use unhosted wallets to remain anonymous and avoid law enforcement detection.

62. With an unhosted wallet, a user needs "gas" to send USDT via the Ethereum or Tron network. Gas is the fee required to successfully conduct a transaction or execute a contract on the Ethereum or Tron blockchain platform. By following the transaction history related to "gas fees," agents can connect individuals associated with unhosted wallets because "gas fees" can generally be traced to a virtual currency exchange that requires KYC. "Gas fees" are also frequently used to demonstrate a relationship between the owners of the two wallets as the "gas

[15] KYC is the process that banks and other financial institutions use, in part, to verify a customer's identity when opening an account.

fees" are akin to an opening deposit of a bank account. It would be highly unusual for someone to provide account opening funds to someone unless they were opening another account for themselves or there was a previous relationship between the two account holders.

Related Address A (address ending in GEvrDQ5K)

63. Related Address A is an unhosted wallet and the owner is unknown at this time. Blockchain analysis shows that Related Address A was activated[16] and received its first incoming transfer of 100 TRX[17] on May 21, 2024, from address ending in C5xctm6V, hereinafter Related Address B. Blockchain records show that between May 16, 2024, and October 17, 2024, Related Address A received a total incoming volume of cryptocurrency transactions worth $11,653,248 and sent transactions totaling $11,653,255 worth of cryptocurrency. The fact that this account address has received and sent similar amounts of cryptocurrency indicates that the address was a pass-through account. Based on their training and experience, agents know that "pass-through" accounts are merely used to pass the cryptocurrency from one address to another to obfuscate the source and destination of the funds.

64. Blockchain analysis shows that as of October 17, 2024, Related Address A had sent cryptocurrency valued at $1,322,815 to Related Address B; $718,765 to Related Address D; $15,001 to Related Address E; $99,984 to Related Address G; $19,998 to Related Address H; and, from June 19, 2024, through August 13, 2024, had sent cryptocurrency valued at $157,936 to Subject Address Vs7by2cS.

[16] An address on the TRON network is considered activated when it receives at least 0.1 TRX from another address.

[17] "Gas" fees on the TRON network are paid with TRX cryptocurrency.

65. Blockchain analysis further shows that Related Address A also received cryptocurrency valued at $378,568 from Related Address B, $3 from Related Address D, and, on August 1, 2024, received cryptocurrency valued at $94,934 from Subject Address Vs7by2cS.

66. Based on their investigation to date, agents believe that the transactions were being conducted between addresses controlled by the same owners or by multiple owners to obfuscate the source and destination of funds.

Related Address B (address ending in C5xctm6V)

67. Related Address B is an unhosted wallet and the owner is unknown at this time. Blockchain analysis shows that Related Address B was activated and received 412.346156 TRX on February 12, 2024, by a Binance account belonging to an individual having the initials M.L.F.

68. On May 10, 2024, during a Department of Homeland Security – Homeland Security Investigations (HSI) investigation, a money pickup of $170,000 was conducted from a suspected drug trafficker in Columbus, Ohio. Those funds were converted to cryptocurrency and sent to an address provided by HSI's targeted money broker. From the Broker's address, the funds were divided and sent to four separate addresses. One of those addresses then divided and sent the funds to four addresses, with 100,000 USDT going to Related Address B.

69. Blockchain records show that between February 12, 2024, and October 12, 2024, Related Address B received a total incoming volume of cryptocurrency transactions worth $26,157,076 and sent transactions totaling $26,157,008 worth of cryptocurrency. Again, the fact that this account address had received and sent similar amounts of cryptocurrency indicates that Related Address B was a pass-through account.

70. Analysis of Related Address B shows that on April 16, 2024, it sent 25 TRX and activated address ending in e8VTPFRj, hereinafter "Related Address C."

71. Blockchain analysis shows that Related Address B had sent cryptocurrency valued at $378,568 to Related Address A; $589,678 to Related Address C; $756,917 to Related Address D; $73,970 to Related Address E; $36,339 to Related Address G; $107,082 to Related Address H; and, from April 30, 2024, through September 19, 2024, had sent cryptocurrency valued at $358,939 to Subject Address Vs7by2cS.

72. Blockchain analysis further shows that Related Address B also received cryptocurrency valued at $1,322,815 from Related Address A and $53,231 from Related Address C.

73. Based on their investigation to date, agents believe that the transactions were being conducted between addresses controlled by the same owners or by multiple owners to obfuscate the source and destination of funds.

Related Address C (address ending in e8VTPFRj)

74. Related Address C is an unhosted wallet and the owner is unknown at this time. Blockchain records show that between April 16, 2024, and May 16, 2024, Related Address C received a total incoming volume of cryptocurrency transactions worth $1,074,349 and sent transactions totaling $1,074,561 worth of cryptocurrency. Again, the fact that this account address had received and sent similar amounts of cryptocurrency indicates that Related Address C was a pass-through account.

75. Blockchain analysis shows that Related Address C received cryptocurrency valued at $589,678 from Related Address B.

76. Blockchain analysis further shows that Related Address C had sent cryptocurrency valued at $53,231 to Related Address B; $222,133 to Related Address D; $19,992 to Related Address E; and, from April 25, 2024, through May 15, 2024, had sent cryptocurrency valued at $180,933 to Subject Address Vs7by2cS.

77. Blockchain analysis of Related Address C shows that on May 15, 2024, it sent 320 TRX and activated Related Address D. Additionally, in the hour before activating Related Address D, Related Address C transferred 221,598 USDT to Related Address D. These transfers constituted the remaining balance in Related Address C. Related Address C did not conduct any transactions after that transaction and had essentially been closed since May 15, 2024. Based on their investigation to date, agents believe that Related Address D replaced Related Address C.

78. Based on their investigation to date, agents believe that the transactions were being conducted between addresses controlled by the same owners or by multiple owners to obfuscate the source and destination of funds.

Related Address D (address ending in jm7B4CUn)

79. Related Address D is an unhosted wallet and the owner is unknown at this time. On July 1, 2024, DEA-Chicago agents coordinated a money pickup of $100,000 in bulk currency – suspected proceeds of drug trafficking – in Newark, New Jersey. These funds were deposited into an undercover bank account before a portion of the funds was converted to cryptocurrency and sent to an address provided by DEA-Chicago's money broker. Blockchain analysis shows that after five "hops" through other wallets, 96,000 USDT of DEA-Chicago funds were sent to Related Address D. Approximately 16 minutes later, Related Address D sent 30,000 of those USDT to Subject Address Vs7by2cS.

80. Blockchain analysis shows that between May 15, 2024, and August 27, 2024, Related Address D received a total incoming volume of cryptocurrency transactions worth $2,360,993 and sent transactions totaling $2,360,745 worth of cryptocurrency. Again, the fact that this account address had received and sent similar amounts of cryptocurrency indicates that Related Address D was a pass-through account.

81. Blockchain analysis further shows that Related Address D had sent cryptocurrency valued at $3 to Related Address A; $43,253 to Related Address E; $94,974 to Related Address H; and, from May16, 2024, through August 27, 2024, had sent cryptocurrency valued at $494,064 to Subject Address Vs7by2cS.

82. Blockchain analysis further shows that Related Address D had also received cryptocurrency valued at $718,765 from Related Address A; $756,917 from Related Address B; $222,133 from Related Address C; and $53 from M.L.F.'s Binance account.

83. Based on their investigation to date, agents believe that the transactions were being conducted between addresses controlled by the same owners or by multiple owners to obfuscate the source and destination of funds.

Related Address E (address ending in K8tbWtoo)

84. According to OKX Exchange records, Related Address E is owned by an individual having the initials T.Z., who is a Chinese citizen.

85. Related Address E was also identified during a DEA-Chicago money laundering investigation. On September 6, 2024, DEA-Chicago agents coordinated a money pickup in Atlanta, Georgia, of $75,000 from a suspected drug trafficker. These funds were deposited into undercover bank accounts before a portion of the funds was converted to cryptocurrency and sent to an address provided by DEA-Chicago's money broker.

A. Blockchain analysis shows that after four "hops" through other wallets, 72,150 USDT of those funds were sent to an address ending in 4o62CbUr, hereinafter "Related Address G."

B. Twenty-one minutes later, Related Address G sent 5,000 USDT to address ending in NcabWRCG, hereinafter "Related Address H."

86. Blockchain analysis shows that Related Address G and Related Address H have both interacted with Related Address E.

87. Blockchain analysis further shows that between December 13, 2022, and October 21, 2024, Related Address E received a total incoming volume of cryptocurrency transactions worth $7,172,672 and sent transactions totaling $7,162,613 worth of cryptocurrency. Again, the fact that this account address had received and sent similar amounts of cryptocurrency indicates that Related Address E was a pass-through account.

88. OKX records show that Related Address E had sent cryptocurrency valued at $49,969 to Related Address H and that on May 14, 2024, had sent cryptocurrency valued at $1,683 to Subject Address Vs7by2cS.

89. Blockchain analysis shows that Related Address E had also received cryptocurrency valued at $15,001 from Related Address A; $73,970 from Related Address B; $19,992 from Related Address C; $43,253 from Related Address D; $3,555 from Related Address F; $44,000 from Related Address G; $9,995 from Related Address H; and, on April 5, 2024, received cryptocurrency valued at $3,059 from Subject Address Vs7by2cS.

90. Based on their investigation to date, agents believe that the transactions were being conducted between addresses controlled by the same owners or by multiple owners to obfuscate the source and destination of funds.

Related Address F (address ending in zww93KNg), which activated Subject Address Vs7by2cS

91. Related Address F is an unhosted wallet and the owner is unknown at this time. Analysis of Related Address F shows that on January 18, 2024, it sent 30 TRX and activated Subject Address Vs7by2cS. Approximately two weeks later, on February 5, 2024, Related Address F sent all remaining funds from the address, and Related Address F was essentially closed.

92. Blockchain analysis shows that between May 26, 2023, and February 5, 2024, Related Address F received a total incoming volume of cryptocurrency transactions worth $11,981,693 and sent transactions totaling $11,981,711 worth of cryptocurrency. Again, the fact

that this account address had received and sent similar amounts of cryptocurrency indicates that Related Address F was a pass-through account.

93. Blockchain analysis further shows that Related Address F had sent cryptocurrency valued at $3,555 to Related Address E and also received cryptocurrency valued at $39,998 from Related Address G.

94. Based on their investigation to date, agents believe that the transactions were being conducted between addresses controlled by the same owners or by multiple owners to obfuscate the source and destination of funds.

Related Address G (address ending in 4o62CbUr)

95. Related Address G is an unhosted wallet and the owner is unknown at this time. As described in paragraph 85, following the September 6, 2024, $75,000 money pickup from a suspected drug trafficker that DEA-Chicago agents coordinated in Atlanta, Georgia, blockchain analysis shows that after four "hops" through other wallets, 72,150 USDT of the funds were sent to Related Address G. Twenty-one minutes later, Related Address G sent 5,000 USDT to Related Address H.

96. Blockchain analysis shows that between December 12, 2023, and October 22, 2024, Related Address G received a total incoming volume of cryptocurrency transactions worth $1,633,664 and sent transactions totaling $1,663,446 worth of cryptocurrency. Again, the fact that this account address had received and sent similar amounts indicates that Related Address G was a pass-through account.

97. Blockchain analysis further shows that Related Address G had sent cryptocurrency valued at $44,000 to Related Address E; $39,998 to Related Address F; and $71,938 to Related Address H.

98. Blockchain analysis further shows that Related Address G also received cryptocurrency valued at $99,984 from Related Address A and $36,339 from Related Address B.

99. Based on their investigation to date, agents believe that the transactions were being conducted between addresses controlled by the same owners or by multiple owners to obfuscate the source and destination of funds.

Related Address H (address ending in NcabWRCG)

100. Related Address H is an unhosted wallet and the owner is unknown at this time. As described in paragraph 85, following the September 6, 2024, $75,000 money pickup from a suspected drug trafficker that DEA-Chicago agents coordinated in Atlanta, Georgia, blockchain analysis shows that after four "hops" through other wallets, 72,150 USDT of DEA-Chicago funds were sent to Related Address G. Twenty-one minutes later, Related Address G sent 5,000 USDT to Related Address H.

101. Blockchain analysis shows that between December 27, 2021, and October 23, 2024, Related Address H received a total incoming volume of cryptocurrency transactions worth $13,440,548 and sent transactions totaling $13,414,673 worth of cryptocurrency. Again, the fact that this account address had received and sent similar amounts indicates that Related Address H was a pass-through account.

102. Blockchain analysis further shows that Related Address H had sent cryptocurrency valued at $9,995 to Related Address E.

103. Blockchain analysis further shows that Related Address H also received cryptocurrency valued at $19,998 from Related Address A; $107,082 from Related Address B; $94,974 from Related Address D; $49,969 from Related Address E; and $71,938 from Related Address G.

104. Based on their investigation to date, agents believe that the transactions were being conducted between addresses controlled by the same owners or by multiple owners to obfuscate the source and destination of funds.

Subject Address Vs7by2cS

105. Subject Address Vs7by2cS is an unhosted wallet and the owner is unknown at this time. As noted in paragraph 91, on January 18, 2024, Related Address F sent 30 TRX and activated Subject Address Vs7by2cS. Approximately two weeks later, on February 5, 2024, Related Address F sent all remaining funds from that address, and Related Address F was essentially closed.

106. Blockchain analysis shows that between January 18, 2024, and October 11, 2024, Subject Address Vs7by2cS received a total incoming volume of cryptocurrency transactions worth $4,722,525 and sent transactions totaling $4,263,294 worth of cryptocurrency. Again, the fact that this account address had received and sent similar amounts indicates that Subject Address Vs7by2cS is another pass-through account in this money laundering network.

107. Blockchain analysis further shows that Subject Address Vs7by2cS sent cryptocurrency valued at $94,934 to Related Address A on August 1, 2024, and on April 5, 2024, sent cryptocurrency valued at $3,059 to Related Address E.

108. Blockchain analysis further shows the following:

A. From June 19, 2024, through August 13, 2024, Subject Address Vs7by2cS received cryptocurrency totaling a value of $157,936 from Related Address A;

B. From June 19, 2024, through August 13, 2024, Subject Address Vs7by2cS received cryptocurrency totaling a value of $358,939 from Related Address B;

C. From April 25, 2024, through May 15, 2024, Subject Address Vs7by2cS received cryptocurrency totaling a value of $180,933 from Related Address C;

D. From May 16, 2024, through August 27, 2024, Subject Address Vs7by2cS received cryptocurrency totaling a value of $494,064 from Related Address D; and

E. On May 14, 2024, Subject Address Vs7by2cS received cryptocurrency valued at $1,683 from Related Address E.

109. Based on their investigation to date, agents believe that all of the transactions occurring among Subject Address Vs7by2cS and the Related Addresses appear to lack a legitimate business or investment purpose and were being conducted between addresses controlled by the same owners or by multiple owners to obfuscate the source and destination of funds.

110. Based on their training and experience, and the investigation to date, agents believe that the defendant approximately 459,611.859199 Tether (USDT) cryptocurrency from Subject Address Vs7by2cS is proceeds of drug trafficking that was involved in money laundering.

111. Based on their training and experience, and the investigation to date, agents believe that Subject Address Vs7by2cS was being used to facilitate money laundering.

Warrant for Arrest In Rem

112. Upon the filing of this complaint, the plaintiff requests that the Court issue an arrest warrant *in rem* pursuant to Supplemental Rule G(3)(b), which the plaintiff will execute upon the defendant property pursuant to 28 U.S.C. § 1355(d) and Supplemental Rule G(3)(c).

Claim for Relief

113. The plaintiff repeats and incorporates by reference the paragraphs above.

114. By the foregoing and other acts, the defendant property, approximately 459,611.859199 Tether (USDT) cryptocurrency from cryptocurrency address ending in Vs7by2cS, is traceable to, and is therefore proceeds of, distribution of controlled substances in violation of 21 U.S.C. § 841(a)(1).

115. The defendant approximately 459,611.859199 Tether (USDT) cryptocurrency from cryptocurrency address ending in Vs7by2cS is therefore subject to forfeiture to the United States of America under 21 U.S.C. § 881(a)(6).

116. By the foregoing and other acts, the defendant property, approximately 459,611.859199 Tether (USDT) cryptocurrency from cryptocurrency address ending in Vs7by2cS, (1) was involved in, or is traceable to funds involved in, money laundering transactions and a conspiracy to engage in money laundering in violation of 18 U.S.C. §§ 1956 and 1957; and (2) was involved in, or is traceable to funds involved in, unlicensed money transmitting in violation of 18 U.S.C. § 1960.

117. The defendant approximately 459,611.859199 Tether (USDT) cryptocurrency from cryptocurrency address ending in Vs7by2cS is therefore subject to forfeiture under 18 U.S.C. §§ 981(a)(1)(A) and 984.

WHEREFORE, the United States of America prays that a warrant of arrest for the defendant property be issued; that due notice be given to all interested parties to appear and show cause why the forfeiture should not be decreed; that judgment declare the defendant property to be condemned and forfeited to the United States of America for disposition according to law; and that the United States of America be granted such other and further relief as this Court may deem just and equitable, together with the costs and disbursements of this action.

Dated at Milwaukee, Wisconsin, this 28th day of February, 2025.

Respectfully submitted,

RICHARD G. FROHLING
Acting United States Attorney

By: *s/Elizabeth M. Monfils*
ELIZABETH M. MONFILS
Assistant United States Attorney
Wisconsin Bar No. 1061622
Office of the United States Attorney

Eastern District of Wisconsin
517 E. Wisconsin Avenue, Room 530
Milwaukee, WI 53202
Telephone: (414) 297-1700
Fax: (414) 297-1738
E-Mail: elizabeth.monfils@usdoj.gov

Verification

I, Kellen Williams, hereby verify and declare under penalty of perjury that I am a Special Agent with the Drug Enforcement Administration ("DEA"), that I have read the foregoing Verified Complaint for Civil Forfeiture *in rem* and know the contents thereof, and that the factual matters contained in paragraphs 10 through 111 of the Verified Complaint are true to my own knowledge.

The sources of my knowledge are the official files and records of the United States, information supplied to me by other law enforcement officers, as well as my investigation of this case, together with others, as a Special Agent with the DEA.

I hereby verify and declare under penalty of perjury that the foregoing is true and correct.

Date: 02/28/2025

s/KELLEN WILLIAMS
Kellen Williams
Special Agent
Drug Enforcement Administration